## REMARKS

Reconsideration and allowance of the present application are respectfully requested. Claims 1-35 remain pending in the application. By this Amendment, the specification is amended; claims 3-5, 18, 19, 29 and 30 are amended; and claims 34 and 35 are new.

In view of the Request for Continued Examination filed herewith, Applicants have taken the opportunity to make minor typographic changes to the specification, correcting typographic errors either as originally filed, or as published. Likewise, in order to afford the best possible claims coverage, certain of the claims are amended for minor clarity, and claims 34 and 35 are added. Support for dependent claim 34 can be found in the specification, e.g., at page 18, lines 9-24, page 31, lines 13-25, page 34, lines 3-27; and support for dependent claim 35 can be found in the specification, e.g., at page 35, lines 3-10.

In numbered paragraph 2, pages 2-14 of the final Office Action, claims 1-15, 19, 22-24 and 26-33 are again rejected as being anticipated by U.S. Patent 6,301,658 (Koehler). In numbered paragraph 4, pages 14-16 of the final Office Action, dependent claims 16-18 are again rejected as being unpatentable over Koehler in view of U.S. Patent 4,264,782 (Konheim). In numbered paragraph 5, pages 16-17 of the final Office Action, dependent claims 20 and 21 are again rejected as being unpatentable over the Koehler patent in view of U.S. Patent 5,903,651 (Kocher). In numbered paragraph 6, page 17 of the final Office Action, dependent claim 25 is again rejected as being unpatentable over the Koehler patent in view of U.S. Patent 5,818,955 (Smithies et al.). These rejections are respectfully traversed.

Applicants have previously made of record Applicants' arguments against the prior art rejections, succinctly reciting the claimed features being argued, and pointing out the support found in the specification for the salient aspects of the argument. The present Remarks by the Applicants are directed to traverse the new assertions made of record by the Examiner in making his obviousness-based rejections in the outstanding final Office Action. The prior-art rejections are traversed at least for the reasons as previously set forth, and as succinctly set forth below.

**Summary of Applicants' Traversals: Response to Arguments**

In defending the outstanding rejections, the Examiner has made of record Response to Arguments in pages 18-28 of the final Office Action. Applicants respectfully submit that the Examiner has misapplied the Koehler patent with regards to what Applicants have claimed. The Examiner's applied references do not address similar means or capabilities. In many instances the Examiner appears to focus on commonality of words, rather than what is the subject of the reference and what is really being described. The Examiner attributes and extends the disclosure of the Koehler patent in ways that were not intended, not known to one skilled in the art at the time, and that deviate from the Internet PKI standards in use at the time.

The Examiner appears to disregard much of our earlier Office Action Remarks of record that clearly argued the differences between the Applicants' claimed features and the Koehler patent as applied by the Examiner. Instead, the Examiner appears to focus on words and sentences in the Koehler patent, disregarding the context of the disclosure. For example, the Examiner appears to equate Applicants' claimed 'trusted third-party repository of information objects' with the Koehler

'certificate server'. These two features perform entirely different functions with no feature overlap.

The objective of the Koehler patent was to reduce the computational and communications overhead of retrieving and verifying status of a certificate using a CRL issued by an organization's CA hierarchy (PKI). Economies are presented for verifying the hierarchy's certificate chain, retrieving and scanning CRLs, caching client certificate status, and updating cache when a newer CRL becomes available. When queried, the Koehler verification server simply reports current certificate status which is used when a client verifies another client's digital signature. Only the verification server performs CRLs and CA hierarchy certificate chain processing. Trust is never an issue since the verification server only operates within the organization that owns and/or controls the CA hierarchy.

The PKI environment on the Intranet has become very complex since the Koehler patent disclosure. A large number of independent CAs and CA hierarchies (PKIs) exist today evidenced by the number of CA certificates cached in a browser's CA certificate store. These CAs employ both off-the-shelf (e.g., Baltimore UniCert CA, Entrust CA, RSA Keon CA) and proprietary (e.g., GTE CyberTrust, Thawte, VeriSign) software, systems, standards and certificate status reporting means. Commercial and government CAs establish multiple trust levels for issuing certificates to subscribers. The trust levels are meant to reflect risk; i.e., the confidence or lack of confidence in the procedures employed to prove the identity of the party/entity purchasing/requesting the certificate. Banks and Credit Card Companies have attempted to overcome some the technical and trust issues by creating proprietary PKI standard based environments such as required by the

Secure Electronic Transaction (SET) specification. Organizations need to be able to control which CA issued certificates are allowable and for what purposes they can be used, regardless of whether the certificates are valid. This is one of the goals of the Bisbee invention.

In contrast, Applicants' disclosure, as broadly encompassed by the claims, seeks to solve the CA inter-working and trust issues that exist when attempting to verify digital signatures based on certificates issued by an organization's or another organizations CA/PKI, or by an independent CA/PKI. Applicants' CSS goes well beyond the Koehler patent disclosure by addressing the methods to work concurrently with or reject any CA or PKI, not dependent on what policies, practices, procedures, and certificate status reporting means are employed.

Applicants' disclosure provides controls that manage and govern acceptance of independent CAs, CAs within hierarchies, and CA issued certificates. For example:

As broadly encompassed by claim 3, individual CAs are identified to the CSS as trusted (certificates accepted) or untrusted (certificates not accepted). This feature is used to restrict or allow CA's based on a client's organization business needs. Where a CAs' issued certificates may be acceptable to one organization for a given type or level of transaction, but not to another.

As broadly encompassed by claim 4, means is provided to force re-approval of a CA and its issued certificates independent of the CA's certificate validity period. A CA's certificate may be valid for 2 to 5 years, but the approving organization may set a time limit after which CA must be reevaluation. The decision to continue or

withdraw approval for a CA is based on the client organizations policies at that time and its experience with that CA's subscribers.

As broadly encompassed by claim 10, CSS is allowed to employ other means of identification such as attribute certificate and/or to consider membership, affiliation and other qualifiers when reporting subscriber certificate status back to a client. Claim 10 also allows the CSS to accept or reject individual self-signed certificates. These certificates are not issued by a CA.

As broadly encompassed by claim 15, limits are placed on the level of activity (number of queries) allowed for a given certificate or to bridge communications outages that do not allow certificate status updates to take place.

The applied references would not have taught or suggested at least the claimed features as set forth. Further specific arguments with respect to key claims 1, 11, 15 and 19 follow. Although claim 19 is a dependent claim, we succinctly argue it's features due to its recitation of like features.

**Claim 1: The Koehler Patent**

Applicants have previously argued of record that the Koehler patent would not have taught or suggested identifying information needed for retrieving a status of an authentication certificate from an issuing CA that issued the authentication certificate, as recited in claim 1.

Regarding claim 1, the Examiner asserts on page 18 of the final Office Action that the Koehler patent discloses "CA digital signature 40 is the digital signature of the issuing certificate authority and is used to verify that certificate 10 is authentic and indeed issued by the authority identified in CA information" and that "the digital

signature provides identifying information from the CA that issued the certificate." Applicants respectfully disagree.

the Koehler patent as applied refers to information contained in a certificate that identifies the issuing CA, the certificates recipient (subject), certificate validity period, and other cryptographic related information necessary to validate the certificate. At the time of the Koehler patent, only CRL based certificate status reporting was supported. Koehler is intended to work within one CA hierarchy where CRL retrieval and processing is well understood and does not require secure connectivity to retrieve CRLs as CRLs are protected.

The identifying information disclosed in Applicants' Claim 1 are the set of protocols and parameters necessary to retrieve certificate status from an approved set of diverse issuing CAs and certificate status responders. A number of certificate status protocols and versions thereof are now in use (e.g., CRL, Online Certificate Status Protocol (OCSP), LDAP schema). The status reporting component may reside separate from the issuing CA and status may be protected with network and/or data security. This information is not contained in a certificate and must be supplied to the CSS separately as per Applicants' claim 1.

There is nothing described in Applicants' specification or claimed that could be interpreted as restricting the CSS so that it would not interoperate with any and all CAs, PKIs and certificate status responders out there. In fact, the claims follow the specification and it should be easily seen that they will achieve the level of interoperability described in the specification. The claims enable the CSS to use multiple connectors to concurrently communicate with numerous CAs, PKIs and certificate status responders to retrieve any type of certificate status. This is

supported in Applicants' published application, at least at paragraphs [0029], [0030], [0057], [0058], [0071], [0087], [0091] & [0104].

It would not have been obvious to extend and scale up the Koehler disclosure to work with multiple CRL based CA hierarchies, let alone multiple independent CAs and certificate status responders. New capabilities would have to be created to manage and keep straight the number of CRLs that would need to be cached and processed.

The Koehler patent discloses retrieving CRLs at specified intervals, or at the times indicated by each CLR's next-update-field. It would be problematic to add the other status protocol capabilities and maintain current certificate status. These other status protocols allow status to be updated at any time and new capabilities would have to be devised and implemented such as those employed by Bisbee to keep and manage the number of updates and resulting statuses from overwhelming Koehler.

At a minimum new CA registration, communication means, certificate status protocols, and cache management capabilities similar to those employed by Bisbee would have to added to Koehler to overcome the physical inter-working issues. In addition, Koehler would still have to solve the Trust issues solved by Bisbee that have limited or stopped all of the many previous government and commercial CA inter-working and PKI bridge activities.

The Examiner asserts that Koehler provides "[v]erification server 60 receives verification requests 90 from a plurality of clients." The Examiner concludes that the server acts as a connector to allow the clients to communicate with the CA based on verification information. Applicants respectfully disagree.

The Koehler disclosure is a "CRL" based verification server (i.e., certificate status responder) that can be queried by a plurality of clients. Koehler, however, cannot retrieve non-CRL based certificate status from multiple different independent CAs and CA hierarchies or where different trust policies are employed. Before Bisbee, there were no inventions that created a trusted CA certificate status bridge or its equivalent.

The Examiner asserts that Koehler provides "[v]erfiication server 60 receives each client request 90 and responds whether a particular digital certificate is authentic." The Examiner concludes that the server communicates when authentication of the certificate is performed. Applicants respectfully disagree.

Applicants' configured connector enable the CSS to concurrently communicate and retrieve all forms of certificate status reporting from any CA, PKI or certificate status responder, regardless of whether they are dependent, independent or use different security and communications technologies or protocols. Koehler only uses CRL and only discloses the communications between the Verification Server its clients. The CRL retrieval means is assumed to be understood. Koehler's stated goal is to reduce communications and computational overhead by caching and reusing a verified certificate's status.

The Examiner asserts that Koehler discloses a server which determines the validity and thus the status of the authentication certificate. Applicants traverse the Examiner's ultimate conclusion.

Koehler only discloses use of the certificate issuer's CRL for obtaining certificate status. The Verification Server caches a certificate's status once obtained to reduce computational overhead. Nowhere does Koehler disclose any mean other

than CRLs and Koehler relies on the fact that CRL retrieval is well understood. Koehler is aimed at improving certificate status performance fairly early in PKI development and deployment. Bisbee solves the problems encountered after dissimilar non-cooperative CAs/PKIs were widely deployed.

**Claim 11: The Koehler Patent**

Regarding claim 11, Applicants have previously argued of record that, among other remarks, the Koehler patent doesn't disclose making use of a time-to-live value, and that the Koehler patent would not have taught or suggested the CSS being used by a trusted third-party repository of information objects for obtaining certificate status, as recited in claim 11.

Regarding claim 11, the Examiner asserts on page 24 of the final Office Action that the Koehler patent provides that the verification server interacts with a certificate repository that may reside across a network and not necessarily connected directly to the server. Applicants respectfully disagree.

The Koehler patent makes no reference that the verification server holds anything other than certificates, CRLs and CRL derived certificate status. The certificate repository is simply a certificate and CRL repository such as the X.500 directory that he references as one embodiment that is a secondary source of this information. Koehler's plurality of clients/applications only requires that the verification server authenticate digital certificates. Koehler neither describes nor discloses any means or method for dealing with any other information object other the certificates, CRL, and certificate status derived from a CRL issued by a single CA hierarchy. The Koehler patent does not suggest any other form of information

object, nor is the verification server shown capable of processing nor managing any other form of information records.

Applicants' CSS, as broadly encompassed by claim 11, supports global commerce applications that inter-work across numerous CA trust domains and therefore requires configurable connectors that can retrieve certificate status using any reporting means from any independent CA, PKI or certificate status reporting service. Further, the Bisbee trusted third-party repository of information objects is in fact 'trusted' to hold documents or negotiable instruments as transferable records that may be authoritative copies. The Koehler patent would not have taught or suggested methods and means that insure that one and only one authoritative copy ever exist, and that this authoritative copy is always held and never released by the trusted third-party repository of information objects. As broadly encompassed by Applicants' claim 11, digital Signatures, where they exist, are validated by the trusted third-party repository of information objects on their submission using certificate status provided by the CSS. At least these features as broadly encompassed by claim 11 would not have been taught or suggested by the Koehler patent.

**Claim 15: The Koehler Patent**

Regarding claim 15, Applicants have previously argued of record that, among other remarks, the Koehler patent would not have taught or suggested the features of providing a status of an authentication certificate as indicated by a Certificate Revocation List ("CRL") when the certificate's issuing CA uses CRLs for indicating status; otherwise, providing the status indicated by a cache memory when the cache memory includes a status and a time-to-live data element is not exceeded; if the time-to-live data element is exceeded, clearing the status from the cache memory;

requesting and retrieving the status using a real-time certificate status reporting protocol when the status is not in the cache memory; adding at least the certificate's identification, status, and time-to-live data element to the cache memory; and providing the retrieved status, as recited in claim 15.

Regarding claim 15, the Examiner asserts on page 25 of the final Office Action that the Koehler patent describes the timestamp being used to determine validity of a certificate. Applicants respectfully disagree.

The Koehler patent relates to the use of a timestamp to indicate whether the CRL is newer than the previously validated certificate; in which case the certificate most be revalidated. Applicants' disclosed time-to-live and other means (e.g., use-counter, last-accessed), as broadly encompassed by claim 15, have nothing to do with knowing when a certificate status has been superseded, but enable the CSS to lower communication overhead, bridge communications outages, force unscheduled status updates, and more affectively manage cache. See, support for the claimed features in Applicant's published application, e.g., at paragraphs [0038], [0039], [0074], [0088] and [0134]. As broadly encompassed by claims 15 (and dependent claims 16 and 17) several means are used by the CSS to reduce the number certificate status queries otherwise required. Time-to-live and use-counter are set by CSS policy and determine when status needs to be updated. Both are set to values required by CSS and policy to meet the level of assurance required for the client's business environment.

Regarding claim 15, the Examiner further asserts on page 25 of the final Office Action that the Koehler patent states that the verification server responds whether a certificate is authentic when a client request is received. The Examiner

then concludes that the status of the issued CA is reported in real time. Applicants respectfully disagree.

The Koehler timestamp is only used to determine whether the validated certificate is fresher that the CRL and can be relied on until the next CRL update. In contrast, when available, Applicants claimed features use a real-time certificate status protocols that guarantee the timeliest of the certificate statuses. Time-to-live and use-count allow Applicants' claimed features to reduce communications overhead by not updating status for every status request. See support found in the Applicants' published application at least at paragraph [0074].

**Claim 19: The Koehler Patent**

Regarding claim 19, Applicants have previously argued of record that, among other remarks, the Koehler patent would not have taught or suggested retrieving an authenticated information object from a trusted repository, according to claim 19 as recited at the time. Applicants respectfully submit that Koehler patent would not have taught or suggested retrieving an authenticated information object from a trusted third-party repository of information objects, wherein the authenticated information object includes a first digital signature block comprising a digital signature of a submitting party and a first authentication certificate relating at least an identity and a cryptographic key to the submitting party, a date and time indicator, and a second digital signature block comprising a second digital signature of the trusted third-party repository of information objects and a second authentication certificate relating at least an identity and a cryptographic key to the trusted third-party repository of information objects; the first digital signature block was validated by the trusted third-party repository of information objects; and the authenticated

information object is stored as an authoritative copy information object under the control of the trusted third-party repository of information objects; executing the retrieved authenticated information object by the second party by including in the retrieved authenticated information object a third digital signature block comprising at least a third digital signature and a third authentication certificate of the second party; and forwarding the executed retrieved authenticated information object to a trusted third-party repository of information objects, wherein the trusted third-party repository of information objects verifies digital signatures and validates authentication certificates associated with the digital signatures included in information objects by at least retrieving status of the authentication certificates from a Certificate Status Service ("CSS") provided according to claim 1, as now recited in claim 19.

Regarding claim 19, the Examiner asserts on page 25 of the final Office Action that the Koehler patent describes the verification server as responding whether a certificate is authentic. The Examiner concludes that 1) the server interacts with a certificate repository that maintains all certificates in the authentication hierarchy; 2) each certificate contains the signature of the issuing authority; and 3) each CA in a hierarchy can validate the certificate of a subordinate CA. Further, timestamps and a CRL allow the repository to determine whether the certificate has been expired or revoked. Applicants respectfully disagree.

The Koehler disclosure does not facilitate the retrieval and execution by a second party of a stored electronic authenticated information object (e.g., transferable record that is an authoritative copy). It does not receive back, further authenticate, reject if authentication fails; otherwise store and control the executed electronic authenticated information object as does the Bisbee trusted third-party

repository of information objects. At most the Koehler disclosure verifies the digital signature applied by the issuing CA to a user authentication certificate and validates the status of the user's certificate when it has been used to create a digital signature. It does not verify digital signatures applied to information objects other than certificates. The Koehler patent is silent with respect to at least the trusted third-party repository of information objects, authoritative copies that may be transferable records, and the protections required for handling authoritative copies. Support for the claimed features can be found in Applicants' published application at least at paragraphs [0019], [0020], [0066] and [0067].

**The Konheim, Kocher and Smithie Patents**

The Konheim, Kocher and Smithie patents do not cure the deficiencies of the Koehler patent. Rather, these secondary references were applied in combination with the Koehler patent to variously reject dependent claims.

Even if combined as the Examiner variously suggested, the Koehler, Konheim, Kocher, and Smithie patents do not combine to result in the claimed features. Although the Examiner variously associate variously disclosed electronic documents in the applied references with Applicants' authenticable information object, the applied references do not disclose the authenticated information object that is the subject of Applicants' claimed features. The claimed features relating to Applicants' authenticated information object are clearly supported by Applicants' specification. Applicants' authenticated information object is an authoritative copy of a transferable record (see support found in Applicants' published application at least at paragraph [0019]). Applicants have realized the legal limitations placed on paper original documents that are transferable records, and Applicants have solved the

problem. This cannot be achieved by combining the Koehler, Konheim, Kocher, and/or Smithie patents as the Examiner has variously suggested.

At least for the foregoing reasons, and as made of record in Applicants' previous Remarks, Applicants' claims 1, 11, 15, and 19 as argued are allowable. The remaining claims depend from the respective independent claims and recite additional advantageous features which further distinguish over the documents relied upon by the Examiner. As such, the present application is in condition for allowance.

All objections and rejections raised in the Office Action having been addressed, it is respectfully submitted that the application is in condition for allowance and a Notice of Allowance is respectfully solicited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: March 30, 2007 By: _____

Richard J. Kim
Registration No. 48360

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620